аудіотрансляції та запису видачі команд ОПР на робочому місці буде отримана аудіоінформація і передана до СЦ об'єкта.

Таблиця 3

Ідентифікація циркулювання інформації в пакеті програмних продуктів

Назва поля	Призначення поля	Тип даних
ansId	Ідентифікатор запитання_відповіді, унікальний номер	Integer
reportId	Ідентифікатор доповіді	Integer
materialId	Ідентифікатор матеріалу	Integer
participantId	Ідентифікатор учасника, який поставив запитання	Integer
linkToAudioFile	Посилання на файл аудіопротоколу (шлях) питання	String
linkToAudioFileAns	Посилання на файл аудіопротоколу (шлях) відповіді	String
ansStartDateTime	Дата/час початку питання	Datetime

Висновки. Впровадження імпульсного вибухопожежного захисту хімічного підприємства вимагає вирішення ряду задач з забезпечення актуальною і своєчасною інформацією ОПР, з метою прийняття обґрунтованих рішень. Саме за цих умов будуть використані всі переваги як імпульсної техніки у порівнянні з традиційною протипожежною технікою, так і всі можливості сучасних програмно-апаратних засобів для відслідковування аварійної ситуації на хімічному підприємстві. Запропонований пакет програмних продуктів забезпечує отримання своєчасної аудіо- та відеоінформації з місця події за умов доступу в локальну чи глобальну мережу, архівування інформації та передачу архівних файлів у відповідну базу даних, а також дозволяє виконати повний цикл проведення нарад в ситуаційному центрі об'єкта для недопущення виходу аварії за межі робочого майданчика.

ЛІТЕРАТУРА

1. Програмний виріб «Система моніторингу стану потенційно небезпечних військових об'єктів». Керівництво користувача. ИКПЛ.466452.011 ИЗ. – Київ: ІПММС НАНУ, 2008 – 70 с.
2. Програмний виріб «Прогнозування та оцінка наслідків катастроф з хімічною речовиною на об'єктах ЗС України». Керівництво з адміністрування. ИКПЛ.466452.009 32. – Київ: ІПММС НАНУ, 2008 – 37 с.
3. Кряжич О.О., Захматов В.Д. Відповідність моделі ППР імпульсної вибухопожежної безпеки потребам підприємства [Текст] / О.О. Кряжич, В.Д. Захматов // Вісник Чернігівського державного технологічного університету. Серія «Технічні науки»: науковий збірник / Черніг. держ. технол. ун-т. – Чернігів: Черніг. держ. технол. ун-т, 2012. – № 3 (59). С. 220-228.
4. Косс В.А. Комплексна інтелектуальна підтримка процедур ситуаційного управління активними об'єктами // Математичні машини і системи. – 2004. - №4. – С. 13-28.
5. Захматов В. Д. Техника многоплановой защиты. — М.: ИПМ АН СССР, 1991. — 124 с.

Надійшла: 26.10.2012 р.

Рецензент: д.т.н., професор Щербак Л.М.

УДК 621.391.7

Яремчук Ю.Є.

ВИКОРИСТАННЯ РЕКУРЕНТНИХ ПОСЛІДОВНОСТЕЙ ДЛЯ ПОБУДОВИ КРИПТОГРАФІЧНИХ МЕТОДІВ З ВІДКРИТИМ КЛЮЧЕМ

У роботі показано можливість використання рекурентних послідовностей для побудови криптографічних методів з відкритим ключем. Представлено метод розподілу секретних ключів відкритим каналом на основі рекурентних V_k^+ та U_k – послідовностей та їх залежностей. Метод може бути покладено в основу для побудови криптографічних перетворень з відкритим ключем різного призначення як то шифрування, автентифікації чи цифрового підписування. Проведено дослідження представленого методу щодо криптостійкості та обчислювальної складності. Дослідження показало, що метод має перевагу перед відомими методами, оскільки при забезпеченні достатнього рівня стійкості він дозволяє встановлювати необхідну криптостійкість залежно від параметру *k*. Щодо обчислювальної складності, то у порівнянні з відомим методом

Діффі-Хеллмана, запропонований метод забезпечує для кожного користувача майже вдвічі меншу складність обчислень, а також має простішу процедуру завдання параметрів.

Ключові слова: інформація, захист інформації, криптографія, криптографічні методи з відкритим ключем, рекурентні послідовності.

Вступ. На сьогодні криптографічні методи застосовуються в системах захисту і додатках різного призначення. При цьому методи з відкритим ключем володіють суттєвою перевагою, оскільки дозволяють один ключ залишати відкритим і доступним будь-кому, хто забажає стати учасником інформаційного обміну. Використання технології відкритого ключа дозволяє ефективно вирішувати задачі різного криптографічного призначення [1] як то шифрування, автентифікації повідомлень чи особи, цифрового підписування тощо.

Вперше можливість побудови криптографічних методів на основі відкритого ключа була запропонована в роботі [2] Діффі та Хеллмана. Суть підходу полягає у використанні дискретного піднесення до степеня для обміну секретними ключами між користувачами мережі з використанням тільки відкритих повідомлень. Пізніше було запропоновано цілий ряд варіантів [3] цього методу.

Запропонований підхід Діффі-Хеллмана в класичному вигляді є недостатньо криптостійкий, оскільки не передбачає перевірки автентичності джерела повідомлень. Для того, щоб ключі були узгоджені лише між двома користувачами необхідно, щоб обидві сторони були впевнені один в одному. Цей недолік може бути усунутий завдяки модифікацій базового методу, наприклад, так як це було показано в роботі [4].

Криптостійкість методу Діффі-Хеллмана базується на складності обчислення дискретних логарифмів, що на сьогодні відноситься до важковирішуваних задач. При цьому проблема дискретного логарифмування досліджується на сьогодні доволі активно, про що свідчать хоча б результати в роботі [5]. Тому пошук та розробка таких математичних апаратів, які могли б стати основою побудови ефективних криптографічних методів з відкритим ключем залишається актуальним.

В цьому зв’язку певний інтерес викликає робота [6] авторів Сміта і Скіннера, які запропонували використовувати рекурентні послідовності Люка за модулем простого числа p замість піднесення до степеня за модулем як це робили Діффі і Хеллман. Хоча в роботі [7] було вказано на певну слабкість підходу запропонованого у роботі [6], це не означає, що рекурентні послідовності як математичний апарат не можуть ефективно використовуватись для побудови криптографічних методів з відкритим ключем. Актуальними є дослідження та пошуки таких послідовностей, які могли б бути ефективно використані для даних криптографічних призначень.

Постановка задачі. Провести дослідження рекурентних послідовностей щодо можливості побудови ефективних криптографічних методів з відкритим ключем та провести оцінювання складності обчислень і криптографічної стійкості такої можливості побудови.

Дослідження рекурентних послідовностей щодо побудови криптографічних методів з відкритим ключем

Рекурентні послідовності в загальному вигляді породжуються таким співвідношенням [8]

$$u_n = a_1 \cdot u_{n-1} + a_2 \cdot u_{n-2} + \ldots + a_k \cdot u_{n-k},$$

де $a_1, a_2, \ldots, a_k$ - коефіцієнти, k - порядок послідовності, виходячи з початкових елементів $u_0, u_1, \ldots, u_k$.

Назвемо послідовність чисел, що обчислюються за формулою

$$v_{n,k} = g_k v_{n-1,k} + g_1 v_{n-k,k} \qquad (1)$$

для початкових значень $v_{0,k} = 1$, $v_{1,k} = g_2$ для $k = 2$; $v_{0,k} = v_{1,k} = \ldots = v_{k-3,k} = 0$, $v_{k-2,k} = 1$, $v_{k-1,k} = g_k$ для $k > 2$; де g_1, g_k – цілі числа; n і k – цілі додатні – V_k^+–послідовністю.

Формула (1) дозволяє отримувати значення для зростаючих n, починаючи з $n = 0$. Можлива і зворотна процедура, коли елементи послідовності обчислюються для спадних n,

починаючи з деякого значення $n = l$. Обчислення елементів такої послідовності буде здійснюватись таким чином

$$v_{n,k} = \frac{v_{n+k,k} - g_k \cdot v_{n+k-1,k}}{g_1}. \quad (2)$$

Для будь-яких цілих додатних n, m та k отримано таку аналітичну залежність

$$v_{n+m,k} = v_{m+(k-2),k} \cdot v_{n,k} + g_1 \cdot \sum_{i=1}^{k-1} v_{m+(k-2)-i,k} \cdot v_{n-k+i,k}. \quad (3)$$

В окремому випадку, коли $m = n$ залежність (3) буде мати такий вигляд

$$v_{2n,k} = v_{n+(k-2),k} \cdot v_{n,k} + g_1 \cdot \sum_{i=1}^{k-1} v_{n+(k-2)-i,k} \cdot v_{n-k+i,k}. \quad (4)$$

Назвемо послідовність чисел, що обчислюються за формулою

$$u_{n,k} = g_k u_{n-1,k} + g_1 u_{n-k,k} \quad (5)$$

для початкових значень $u_{0,k} = g_1$, $u_{1,k} = g_2$, $u_{2,k} = g_3$, ... $u_{k-1,k} = g_k$; де g_1, g_2, g_3, ..., g_k – цілі числа; n і k – цілі додатні числа – U_k–послідовністю.

Для будь-яких цілих додатних n, m та k отримано таку залежність

$$u_{n+m,k} = v_{m+(k-2),k} \cdot u_{n,k} + g_1 \cdot \sum_{i=1}^{k-1} v_{m+(k-2)-i,k} \cdot u_{n-k+i,k}. \quad (6)$$

Для будь-яких цілих додатних n та k, таких що $n \geq k$, отримано залежність, яка дозволяє обчислювати елементи U_k–послідовності тільки на основі елементів V_k^+–послідовності

$$u_{n,k} = g_k \cdot v_{n-1,k} + g_1 \cdot \sum_{i=1}^{k-1} g_i \cdot v_{n-i-1,k}. \quad (7)$$

Представлені рекурентні послідовності, а також отримані залежності дозволяють виконувати криптографічні перетворення з відкритим ключем. Розглянемо метод розподілу секретних ключів відкритим каналом на основі запропонованого математичного апарату. Даний метод може стати основою для побудови криптографічних методів різного призначення, основаних на технології відкритого ключа.

Ідея методу, що пропонується, базується на властивості (6), яка дозволяє обчислити елемент $u_{n+m,k}$ використовуючи елементи V_k^+ та U_k–послідовностей, причому зробити це двома шляхами: або використовуючи елементи $v_{m+i,k}$, $i = \overline{-1, k-2}$, та $u_{n-i,k}$, $i = \overline{0, k-1}$, або використовуючи елементи $v_{n+i,k}$, $i = \overline{-1, k-2}$, та $u_{m-i,k}$, $i = \overline{0, k-1}$.

Тоді, якщо один користувач для будь-якого вибраного їм випадкового числа a обчислить $u_{a-i,k}$, $i = \overline{0, k-1}$, а другий користувач аналогічним чином обчислить $u_{b-i,k}$, $i = \overline{0, k-1}$, то, обмінявшись обчисленими значеннями, кожен з них зможе отримати $u_{a+b,k}$, продовжуючи обчислення на своєму боці за формулою (6), використовуючи відповідно свої числа a або b. В цьому випадку $u_{a+b,k}$ буде ключем розподілу, а числа a і b секретним ключем кожного користувача. Причому, a і b - це частини секретного ключа кожного користувача, оскільки попереднє отримання ключа розподілу будь-яким користувачем не можливе без отримання відповідної інформації від іншого користувача.

Операція за модулем в схемі розподілу ключів використовується для обмеження розрядності чисел під час виконання арифметичних операцій.

Відповідно до запропонованого методу основні обчислення виконуються за формулою (6). Для обчислення елементу $u_{n+m,k}$ за цією формулою потрібні елементи $v_{m+i,k}$, $i = \overline{-1, k-2}$, та елементи $u_{n-i,k}$, $i = \overline{0, k-1}$. Обчислення останнього набору елементів здійснюється за формулою (7), для чого необхідно мати елементи $v_{n+i,k}$, $i = \overline{-2k+1, -1}$. Звідси

виходить, що всього для обчислення елементу $u_{n+m,k}$ за формулою (6) потрібно мати елементи $v_{n+i,k}$, $i=\overline{-2k+1,k-2}$. Задача знаходження цих елементів зводиться до отримання будь-яких послідовних k з них, оскільки інші можуть бути обчислені за формулами (1) або (2) на основі вже отриманих.

Виходячи з цього схема розподілу ключів відкритим каналом буде мати такий вигляд:

Вибір параметрів
k, p, g_i, $i=\overline{1,k}$

Користувач A вибирає випадкове число a		Користувач B вибирає випадкове число b
Користувач A обчислює за модулем p $u_{a-i,k}$, $i=\overline{0,k-1}$	⟷	Користувач B обчислює за модулем p $u_{b-i,k}$, $i=\overline{0,k-1}$
Користувач A обчислює ключ K $K=u_{b+a,k} \bmod p$		Користувач B обчислює ключ K $K=u_{a+b,k} \bmod p$

Проблема обчислення елементу $v_{n,k}$ полягає в тому, що для великих значень n, а саме такі значення повинні використовуватись в криптографічних перетвореннях, обчислення $v_{n,k}$ за формулою (1) є неприйнятним. Потрібен більш швидкий метод обчислення елементу $v_{n,k}$ з боку санкціонованого користувача.

В зв'язку з цим пропонується спосіб обчислення $v_{n,k}$, який базується на тій же ідеї, що і бінарний метод [9] піднесення до степеня. Скористаємось даним методом для отримання адитивного ланцюжка

$$1 = c_0, c_1, c_2, ..., c_t = n.$$

Якщо записати n в двійковій системі числення як $n=\sum_{i=0}^{t}\alpha_{t-i}2^{t-i}$, то для кожного $i=\overline{1,t}$ правило отримання адитивного ланцюжка, починаючи з c_1, буде таким

- якщо значення α_{t-i} дорівнює 0, то $c_i = 2c_{i-1}$;
- якщо значення розряду α_{t-i} дорівнює 1, то $c_i = 2c_{i-1}+1$.

Як наслідок, дійшовши до крайнього правого розряду n отримаємо $c_t = n$.

Звідси, обчислення $v_{n,k}$ буде зводитись до послідовного обчислення $v_{c_i,k} = v_{2c_{i-1}+1,k}$ або $v_{c_i,k} = v_{2c_{i-1},k}$.

Обчислення $v_{c_i,k} = v_{2c_{i-1},k}$ будемо здійснювати за формулою (4), а $v_{c_i,k} = v_{2c_{i-1}+1,k}$ будемо отримувати, обчислюючи спочатку $v_{2c_{i-1},k}$, а потім $v_{2c_{i-1}+1,k}$ за формулою (1).

З (4) видно, що для отримання елементу $v_{2n,k}$ використовуються елементи $v_{n+k-2,k}$, ..., $v_{n-(k-2),k}$, $v_{n-(k-1),k}$. Тобто на кожному кроці необхідно визначати та зберігати набір з $2k-2$ елементів. Розглянемо обчислення цих елементів.

Елементи $v_{2n,k}$, $v_{2n-1,k}$, ..., $v_{2n-(k-3),k}$, $v_{2n-(k-2),k}$ можуть бути обчислені за формулою (3) відповідно як $v_{n+n,k}$, $v_{n+(n-1),k}$, ..., $v_{n+(n-(k-3)),k}$, $v_{n+(n-(k-2)),k}$.

Елемент $v_{2n-(k-1),k}$ не може бути обчислений за формулою (3), оскільки для його обчислення, окрім елементів, які є в наведеному вище наборі, потрібен елемент $v_{n-k,k}$. Розширення цього набору елементів елементом $v_{n-k,k}$ не бажано, тому що для обчислення

$v_{2n-k,k}$ буде потрібен елемент $v_{2n-(k+1),k}$. Щоб усунути цей недолік будемо обчислювати елемент $v_{2n-(k-1),k}$ за формулою (2).

В такому випадку необхідним є елемент $v_{2n+1,k}$. Цей елемент може бути обчислений за формулою (3). При цьому набір необхідних елементів буде розширений елементом $v_{n+k-1,k}$.

Елементи $v_{2n+k-1,k}$, ..., $v_{2n+3,k}$, $v_{2n+2,k}$ можуть бути отримані на основі вже обчислених елементів $v_{2n+1,k}$, $v_{2n,k}$, ..., $v_{2n-(k-3),k}$, $v_{2n-(k-2),k}$ за формулою (1).

Таким чином, для обчислення елементу $v_{2n,k}$ на кожному кроці необхідно визначати та зберігати набір з $2k-1$ елементів.

Позначивши l, як поточне значення індексу елементу V_k^+–послідовності, маємо такий алгоритм прискореного обчислення елементів цієї послідовності для додатних n.

П.1. Провести початкову ініціалізацію: $i \leftarrow t$; $l \leftarrow 1$; присвоїти елементам $v_{l+k-1,k}$, ..., $v_{l-(k-2),k}$, $v_{l-(k-1),k}$ відповідні значення V_k^+–послідовності.

П.2. $i \leftarrow i-1$.

П.3. $l \leftarrow 2l$.

П.4. Обчислити нові значення $v_{l+1,k}$, $v_{l,k}$, ..., $v_{l-(k-3),k}$, $v_{l-(k-2),k}$ за модулем p, використовуючи (3).

П.5. Обчислити елемент $v_{l-(k-1),k}$ за модулем p, використовуючи (2).

П.6. Якщо $k > 2$, то обчислити елементи $v_{l+k-1,k}$, $v_{l+k-2,k}$, ..., $v_{l+3,k}$, $v_{l+2,k}$ за модулем p, використовуючи (1).

П.7. Якщо $\alpha_i = 0$, то перейти до п.10.

П.8. $l \leftarrow l+1$.

П.9. Обчислити нові значення $v_{l+k-1,k}$, ..., $v_{l-(k-2),k}$, $v_{l-(k-1),k}$ шляхом присвоювання кожному попередньому елементу значення наступного за ним елементу та обчислення за модулем p останнього елементу $v_{l+k-1,k}$ за формулою (1), використовуючи тільки-но обчислені елементи.

П.10. Якщо $i-1 \neq 0$, то перейти до п.3, інакше завершити роботу алгоритму.

Визначивши обчислення за усіма формулами, що використовуються в запропонованому методі розподілу ключів, протокол розподілу ключів відкритим каналом буде мати такий вигляд.

П.1. Задати параметр k.

П.2. Вибрати p.

П.3. Вибрати $g_1, g_2, ..., g_k$.

П.4. Опублікувати параметри.

П.5. Користувачу A вибрати випадкове число a, а користувачу B вибрати випадкове число b.

П.6. Користувачу A обчислити за модулем p $v_{a+i,k}$, а користувачу B обчислити за модулем p $v_{b+i,k}$ для $i = \overline{-(k-1), k-2}$ за алгоритмом прискореного обчислення елементів V_k^+–послідовності.

П.7. Користувачу A обчислити за модулем p $v_{a+i,k}$, а користувачу B обчислити за модулем p $v_{b+i,k}$ для $i = \overline{-2k+1, -k}$ за формулою (2).

П.8. Користувачу A обчислити за модулем p $u_{a-i,k}$, а користувачу B обчислити за модулем p $u_{b-i,k}$ для $i = \overline{0, k-1}$ за формулою (7).

П.9. Користувачу A передати $u_{a-i,k}$ користувачу B, а користувачу B передати $u_{b-i,k}$ користувачу A, де $i = \overline{0, k-1}$.

П.10. Користувачу A обчислити ключ K за формулою

$$K = u_{b+a,k} \bmod p,$$

а користувачу B обчислити ключ K за формулою

$$K = u_{a+b,k} \bmod p,$$

де $u_{b+a,k}$ та $u_{a+b,k}$ обчислюються за формулою (6).

В п.2 протоколу проводиться вибір параметру p, який є модулем при обчисленнях в представленому алгоритмі та визначає верхню межу діапазону чисел, що отримуються під час цих обчислень.

В п.3 протоколу відбувається вибір параметрів g_i, $i = \overline{1,k}$. Оскільки значення будь-якого числа в розробленому алгоритмі обмежується параметром p, вказані параметри слід вибирати в діапазоні $[1, p-1]$. При цьому вибір можна здійснювати за допомогою будь-якого генератора випадкових чисел у вказаному діапазоні.

Оцінювання складності обчислень та криптографічної стійкості запропонованого підходу на основі рекурентних послідовностей

Не важко помітити, що Користувач A і Користувач B виконують за алгоритмом прискореного обчислення елементів V_k^+–послідовності однакову кількість арифметичних операцій над великими числами. Тому для визначення складності обчислень за цим алгоритмом достатньо визначити складність обчислення з боку одного з них, а потім подвоїти отримане значення.

Складність обчислень за алгоритмом прискореного обчислення елементів V_k^+ –послідовності з боку Користувача A визначається складністю обчислень за модулем p елементів $v_{a+i,k}$, $i = \overline{-(k-1),k-2}$, елементів $v_{a+i,k}$, $i = \overline{-2k+1,-k}$, за формулою (2), елементів $u_{a-i,k}$, $i = \overline{0,k-1}$ за формулою (7), та елементу $u_{b+a,k}$ за формулою (6). Обчислення першого набору елементів буде складати приблизно $H^2 q \cdot [6H(k^2+k) + 3(3k^2+k)]$ операцій над машинними одиницями інформації, де H – кількість машинних одиниць інформації для зберігання великого числа, q – кількість розрядів машинної одиниці інформації.

Обчислення інших елементів V_k^+ та U_k – послідовностей за модулем p за формулами (2), (6) та (7) потребує виконання приблизно $k^2 + 4k$ множень, k^2 додавань та k віднімань над машинними одиницями інформації. Враховуючи оцінки складності виконання арифметичних операцій за модулем над числами великої розрядності, складність обчислень за формулами (2), (6) та (7) буде складати приблизно $6H(H+1)(k^2+4k) + 2Hk^2(H+1) + 3Hk(H+1)$ операцій над машинними одиницями інформації. Виходячи з того, що під час реалізації криптографічних методів в сучасних комп'ютерних системах оперують ключами, що мають розмір 1024 і більше розрядів ($Hq \geq 1024$), отримана оцінка буде значно меншою за оцінку складності обчислення набору елементів $v_{a+i,k}$, $i = \overline{-(k-1),k-2}$, а тому може не враховуватись в загальній оцінці складності всього алгоритму розподілу ключів. Таким чином складність виконання запропонованого алгоритму розподілу секретних ключів з боку одного користувача складає приблизно $H^2 q \cdot [6H(k^2+k) + 3(3k^2+k)]$ операцій над машинними одиницями інформації.

Порівнюючи запропонований метод розподілу ключів з відомим методом Діффі-Хеллмана відносно складності виконання розподілу ключів слід відзначити таке. В запропонованому методі обом користувачам необхідно виконувати обчислення певного елементу U_k – послідовності по одному разу, в той час як за методом Діффі-Хеллмана їм необхідно виконувати піднесення до степеня по два рази. При цьому складність обчислення певного елементу U_k – послідовності має той же порядок, що і складність піднесення до заданого степеня. Тому можна стверджувати, що представлений метод має приблизно вдвічі

меншу складність обчислень, ніж метод Діффі-Хеллмана. Крім того, запропонований метод має значно простішу процедуру завдання параметрів, оскільки їх вибір не потребує проведення складних обчислень над великими числами.

Визначимо теоретичну криптостійкість запропонованого методу розподілу ключів за допомогою теоретико-складносного підходу. Для цього визначимо, по-перше, що запропонований метод використовує фіксовані значення параметрів k, q, H, наприклад $k=3$, $q=16$, $H=32$, а параметр безпеки – будь-яке натуральне число. По-друге, будемо вважати, що зловмиснику відома така інформація: протокол розподілу ключів; параметри протоколу k, p, g_i, $i=\overline{1,k}$; елементи $u_{a-i,k} \bmod p$, $i=\overline{0,k-1}$, або $u_{b-i,k} \bmod p$, $i=\overline{0,k-1}$, що передаються відкритим каналом від одного користувача до іншого в процесі розподілу ключів. По-третє, об'єм обчислень будемо вважати «практично нездійсненим», якщо найкращий алгоритм, який буде використовувати зловмисник для зламу, буде виконуватись не за поліноміальний час. Доведемо, що не існує поліноміальних алгоритмів для зламу запропонованого методу. Виходячи з тієї інформації, яка відома зловмиснику, основні його спроби можуть бути спрямовані на отримання секретного значення a або b відповідно з відомих елементів $u_{a-i,k} \bmod p$, $i=\overline{0,k-1}$, або $u_{b-i,k} \bmod p$, $i=\overline{0,k-1}$. Розглянемо можливі спроби зловмисника на основі інформації, яка буде надходити від користувача A, оскільки, очевидно, що спроби з використанням інформації від користувача B будуть аналогічними.

Перше, що може спробувати зловмисник, – отримати секретне значення a шляхом послідовних обчислень за модулем p за формулою (5), доки не буде отримано значення $u_{a,k} \bmod p$. Аналіз показує, що такі обчислення потребують виконання $3aH(4H+5)$ операцій над машинними одиницями інформації. Тобто, якщо продуктивність комп'ютера дорівнює 2^{34} операцій за секунду, для представлення a використовують 1024 розряди, $H=32$, то для виконання цих операцій потрібно приблизно 2^{979} років, що є практично нездійсненим.

Оскільки елементи $u_{a-i,k} \bmod p$, $i=\overline{0,k-1}$, відомі, то можлива спроба знаходження елементів $v_{a+i,k}$, $i=\overline{-(k-1),k-2}$, використовуючи формулу (7). Реалізація цієї спроби зводиться до розв'язання системи з k рівнянь та $k+1$ невідомими. Математична задача розв'язання такої системи рівнянь, враховуючи велику розрядність коефіцієнтів та невідомих, на цей день не має ефективного поліноміального алгоритму, а отже є практично нездійсненою.

Таким чином, злам запропонованого методу розподілу ключів не може бути виконаний за поліноміальний час, а, отже, запропонований метод є теоретично стійким.

Слід також зазначити, що запропонований протокол розподілу ключів дає можливість змінювати параметр k, що дасть змогу підвищувати криптостійкість за рахунок збільшення складності виконання протоколу.

Висновки. Проведено дослідження рекурентних послідовностей щодо можливості побудови криптографічних методів з відкритим ключем. Отримано залежності для V_k^+ та U_k – послідовностей, на основі яких запропоновано метод розподілу секретних ключів відкритим каналом. Запропонований метод може стати основою для побудови криптографічних методів різного призначення, основаних на технології відкритого ключа, як то шифрування, автентифікації чи цифрового підписування. Дослідження представленого методу розподілу ключів щодо криптографічної стійкості показало, що з точки зору теоретичної стійкості метод є стійким. При цьому метод має перевагу перед відомими методами, оскільки дозволяє встановлювати необхідну криптостійкість залежно від параметру *k*. Дослідження обчислювальної складності представленого методу показало, що,

в порівнянні з відомим методом розподілу ключів Діффі-Хеллмана, запропонований метод забезпечує для кожного користувача майже вдвічі меншу складність обчислень. Крім того, запропонований метод має простішу процедуру завдання параметрів.

ЛІТЕРАТУРА

1. Menezes A.J., van Oorschot P.C., Vanstone S.A. Handbook of Applied Cryptography. - CRC Press, 2001. 816 p.
2. W. Diffie, M.E. Hellman. New directions in cryptography // IEEE Transactions on Information Theory. – №22, 1976. – Pp. 644–654.
3. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. - М.: Триумф, 2002. - 816 с.
4. W. Diffie, P.C. van Oorschot, M.J. Wiener. Authentication and authenticated key exchanges // Designs, Codes and cryptography. – №2, 1992. – Pp. 107–125.
5. A.M. Odlyzko. Discrete logarithms: the past and the future // Designs, Codes and Cryptography. – №19, 2000. – Pp. 129–154.
6. Smith P. and Skinner C. A public-key cryptosystem and a digital signature system based on the Lucas function analogue to discrete logarithms // In Advances in Cryptology Asiacrypt ’94, Springer-Verlag. – 1995. – Pp. 357–364.
7. Bleichenbacher D., Bosma W., and Lenstra A. Some remarks on Lucas-based cryptosystems // In Advances in Cryptology Crypto ’95, Springer-Verlag. – 1995. – Pp.386–396.
8. Маркушевич А.И. Возвратные последовательности. - М.: Наука, 1975. - 48 с.
9. Кнут Д. Искусство программирования для ЭВМ, том 2. Получисленные алгоритмы. - М.: Вильямс, 2004.- 832 с.

Надійшла: 18.10.2012 р.

Рецензент: д.т.н., професор Хорошко В.О.

УДК 004.056.53(045)

Стасюк А.И., Корченко А.А.

МЕТОД ВЫЯВЛЕНИЯ АНОМАЛИЙ ПОРОЖДЕННЫХ КИБЕРАТАКАМИ В КОМПЬЮТЕРНЫХ СЕТЯХ

Одним из решений обеспечения безопасности, являются системы обнаружения вторжений, построенные по аномальному принципу. Такие системы обычно основываются на математических методах, требующих много времени на подготовку статистических данных. Поэтому необходимы более эффективные методы, основанные на экспертных подходах. Для решения этой задачи предлагается метод, базирующийся на математических моделях и методах нечеткой логики, и содержащий восемь базовых этапов (выбор метода обработки нечетких данных, выбор метода определения коэффициента важности, формирование множеств атак и параметров, формирование эталонов параметров, фаззификация параметров, формирование множества эвристических правил, определение матриц инициализации, формирование результата), раскрывающие процесс выявления аномального состояния, порождаемого определенным типом кибератак в ИС. Этот метод можно использовать для создания или усовершенствования существующих систем выявления кибератак в компьютерных сетях.

Ключевые слова: кибератака, системы обнаружения вторжений, атаки в компьютерных системах, обнаружение аномалий в компьютерных системах, эвристические правила, базовая модель параметров, универсальная модель эталонов, модель эвристических правил, построение решающих правил, метод обнаружения аномалий, метод обнаружения атак.

Интенсивное развитие информационных технологий оказало положительное влияние на все сферы человеческой деятельности. Вместе с этим наблюдаются и побочные эффекты, в первую очередь в связи с тем, что ресурсы информационных систем (РИС) все больше подвергаются воздействиям кибератак, под которыми понимаются меры, предпринимаемые для подрыва безопасности информационной системы (ИС) или реализация угроз характеристикам безопасности РИС посредством использования их уязвимостей. Современный спектр атак на РИС достаточно широкий и только основываясь на базовые признаки их можно классифицировать по: автоматизации; взаимодействию с политикой безопасности; дистанционности; действию, порожденному несанкционированным доступом; внешнему проявлению; инициализационному условию; инструментальным средствам; наличию обратной связи; нарушению базовых характеристик безопасности; природе